Information Security Management Office
Truman Building, Suite 280

FrontLine

TIPS AND TECHNIQUES TO PROTECT YOUR INFORMATION SYSTEMS

Spring 2002

INSIDE

Don't lose your job to the shadow world

No one saw the Net abuse crackdown coming. A single complaint from a co-worker started it all. By the time it was over, 39 Dow Chemical workers, many of them long-time employees, had lost their jobs, and another 200 had been severely reprimanded and forced to take unpaid leaves of absence. But that wasn't really the end of it. After the company's investigators finished up at a factory in Midland, Michigan, they started a probe at a plant in Freeport, Texas–again, initiated with a single complaint. The toll? Well, 22 more people were fired (18 of them union members); 240 more people were disciplined.

The story received national attention. An expose in the *Los Angeles Times* put human faces on the stark facts of firings and disciplinary actions.

"The first taps on the shoulder came in July, when dozens of workers were summoned to the Dow administration building. They were confronted with incriminating e-mail from their files, suspended for two weeks and told to call in every day for updates. Their hearts would pound as they dialed in each morning. When they were finally summoned back near the end of their suspensions, many assumed they were to return to work. Some braced for the worst they could imagine: suspensions that would be measured in months.

"But the scene at the administration building told a different story. One by one, workers emerged with glazed looks. In the parking lot, women consoled sobbing husbands. Some workers were so distraught that the union had to round up volunteers to drive them home."

John Blanck, 50, was a machinist at the Midland site. He had worked for Dow Chemical for 25 years. He was fired for sending lewd e-mail messages.

"If you want to believe I'm a pornography person or whatever, go ahead. But my morals have always been good. And I would never have even looked at e-mail if I thought it would have meant my job."

Tom Pembroke, 46, had worked in Dow's packaging department since 1989. He was fired for sending an e-mail message that included a pornographic picture.

"Pembroke says that as he sat down for his meeting, his longtime supervisor avoided eye contact and began reading a terse termination letter. 'You guys are making a mistake,' Pembroke pleaded. 'I used bad judgment. Consider my record!' He drove the 15 miles back to his home in a stupor. His wife was still asleep in bed when he rushed to the bathroom and vomited."

There was no warning. Many of the fired workers said in hindsight that a warning would have put an end to the Net abuse. But Dow insists that the workers should have known better and been forewarned.

A 30-page booklet entitled "Respect and Responsibility," which outlines the company's harassment policies had been mailed to employees two months before the investigation. On Page 5, the following item is included in a list of behaviors that Dow will not allow: "utilizing e-mail . . . to view or pass along inappropriate material (particularly relative to race, ethnicity, gender, disability, religion, or of a sexual nature)."

Of course, many workers said they never received "Respect and Responsibility." Others said that they simply sent it to the round file without reading it.

Neither excuse helped the unlucky ones avoid termination.

Organizations are taking the Net abuse problem very seriously.

According to the American Management Association, seventy-three percent of U.S. businesses monitored their employees' Internet use last year.

Organizations are cracking down harder than ever.

Websense, an Internet filtering provider, reports that nearly two-thirds of U.S. companies disciplined workers for misusing the Internet while working, and a third of them—ranging in size from 6 to over 150,000 employees—have terminated workers that use the Internet to loaf.

Organizations are spending lots of money on the crackdown.

International Data Corp. forecasts that the Internet filtering technology market will grow by close to 50% per year, reaching $636 million (707.8 million euros) worldwide by 2004.

And the well-funded crackdown is world-wide.

The Privacy Foundation estimates that the number of employees under such surveillance is at 27 million, just over one-quarter of the global on-line workforce, i.e., those employees who have Internet and/or e-mail access at work, and use it regularly.

In Great Britain, Orange PLC, a mobile phone network subsidiary of France Telecom SA, fired thirty-two workers for distributing pornographic material downloaded from the Internet.

In New Zealand, Justice Robert Fisher and three other judges spent a brief time accessing pornography over the Internet and found themselves in the headlines, subjects of an investigation and under pressure to resign.

In Hungary, the head of parliament's information department installed Internet filters to stop porn being downloaded by members of Parliament and their staffs.

In Canada, a Department of Fisheries and Oceans investigation revealed that its 10,000 employees' visits to sex and dating Web sites averaged about 70,000 hits per day during one week.

The problem isn't simply accessing pornographic sexual content.

The Informa Media Group projects that e-gambling revenue will rise to $14.5 billion worldwide by 2006. Informa believes that by that time, the U.S. will claim 24% of e-gambling revenue, and Europe will claim 53%.

The Society for Human Resource Management reports that 30 percent of employees dive into NCAA office gambling pools. According to PC Data Online, approximately 14 million people visited sports Web sites during last year's NCAA college basketball tournament, aka "March Madness." Websense estimates organizations could suffer $504 million in lost productivity due to employees checking scores and viewing game Webcasts during work hours.

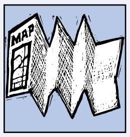
For corporations and government agencies, Net abuse is a problem that affects the bottom line.

The issue isn't morality. The issue is productivity. Whether they are shopping on-line or surfing for film clips of kinky sex, workers get less done if they succumb to the many temptations of the Web.

The issue isn't censorship. The issue is civil liability. What is humorous or sexually arousing to one person is often threatening or offensive to another person. A successfully waged sexual harassment law suit can result in hundreds of thousands or even millions of dollars in damages.

So, faced with the double-whammy of lost productivity and costly legal battles, your enterprise may not hesitate to make an example out of employees who choose to abuse.

Tips on "Net Abuse"



In the absence of a formal, written set of guidelines, adhering to the "Internet Code of Ethics" below should serve you well.

I will…

❒ Protect the organization's information from unauthorized access, modification, duplication, destruction or disclosure

❒ Protect my password as confidential information and not share it with anyone

❒ Only transmit information that has been classified as public

❒ Comply with copyright and software licensing agreements

❒ Report any suspicious activity or suspected compromises of the organization's information systems to appropriate personnel

❒ Scan downloaded files with reliable anti-virus scanning software

I will not…

❒ Download or transmit games, viruses, unlicensed software or offensive materials

❒ Use company-provided Internet access for unauthorized activities

❒ Transmit messages that adversely affect the company's image

❒ Use another person's password to access the Net

❒ Transmit confidential information

Signs of "Netomania"

If, despite your good intentions, you just can't quite get your mind around the "Internet User's Code of Ethics," perhaps you have a psychological problem.

Dr. Kimberly Young, a researcher in the field, has identified several warning signs of excessive Internet use:

❒ Staying on-line longer than you intended

❒ Admitting that you can't keep from or stop signing-on

❒ Neglecting loved ones, chores, sleep, reading, television, friends, exercise, hobbies, sex, or social events because of the Internet

❒ Spending 38 hours or more a week on-line

❒ Failing to cut down on time spent on-line

❒ Feeling anxious, bored, sad, lonely, angry, or stressed before going on-line, but feeling happy, excited, loved, calmed, or confident while on the Internet

❒ Favoring chat rooms, games (particularly, multiuser "Dungeons") over other Internet activities.

E-Mail Security

The following guidelines for responsible e-mail usage were developed for a major corporation with an award-winning information protection program. If you use them as your touchstone, you will most likely avoid running afoul of your own organization's e-mail usage policies and procedures.

Employees who use e-mail should remember:

❒ The e-mail systems of the company are to be used for business purposes only. The company reserves the right to monitor all electronic mail messages.

❒ Any views expressed by individual employees in e-mail messages are not necessarily those of the company.

❒ Any e-mail messages sent to non-employee groups, systems, or individuals must include a disclaimer stating the views of the message are the sender's and do not necessarily represent the views of the company.

❒ Failure to follow your organization's guidelines for appropriate e-mail usage could result in disciplinary action up to and including termination of employment.

Forewarned is forearmed

The most important concept to grasp is the difference between appropriate and inappropriate e-mail usage.

Remember, e-mail is used primarily for business correspondence. Employees should limit their use of e-mail for sending personal messages.

Examples of acceptable uses of e-mail include:

❒ Business messages

❒ Messages about company-sponsored events

❒ Short personal messages deemed necessary (for example, meeting someone for lunch or after work) when calling or physically visiting would take more time

Examples of unacceptable use of e-mail include:

❒ Messages interfering with normal conduct of business

❒ Messages involving solicitation or for-profit personal business activity

❒ Sending chain letters or electronic art

❒ Sending lewd, harassing, or offensive content

What to do and what not to do

Here are some useful tips to avoid possible pitfalls:

❒ Do not share e-mail passwords.

❒ Establish appropriate precautions when sending e-mail. Send information with the assumption that other people may read it.

❒ Establish appropriate precautions when receiving e-mail. If a message is marked confidential, do not send it to other people.

❒ E-mail messages can be made to appear as though they came from someone other than the actual sender (spoofing). When a message is marked confidential or contains sensitive information, call the apparent sender to confirm its origin.

❒ Forward requests you receive for proprietary or confidential information to the area responsible for releasing the information.

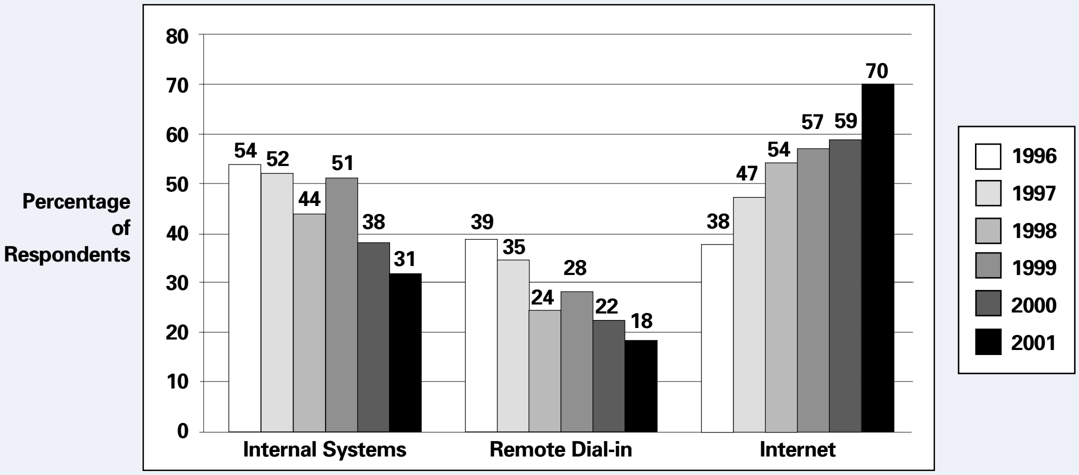
❒ Do not send confidential or proprietary information through a public network such as the Internet or America On-Line (AOL). Use a more secure method, such as the phone, registered mail, or a secure fax to send confidential information.

❒ Do not send or post messages containing medical information on any e-mail system. In the U.S., this practice is against federal regulations and can result in lawsuits.

❒ Messages sent to public newsgroups, listservs, or other public discussion forums must have the following disclaimer: *Any opinions expressed in this message are not necessarily those of the company.*

Proof-Positive

Internet Connection is Increasingly Cited as a Frequent Point of Attack



2001: 384 Respondents/72%
2000: 443 Respondents/68%
1999: 324 Respondents/62%
1998: 279 Respondents/54%
1997: 391 Respondents/69%
1996: 174 Respondents/40%

CSI/FBI 2001 Computer Crime and Security Survey
Source: Computer Security Institute

Horror Stories

Headlines throughout the world abound with tales of cyberspace crimes, misdemeanors, blunders, lapses and snafus. These real-world horror stories make the diverse threats to your organization tangible and poignantly clear.

New York Times Internal Network Hacked

Security holes in the *New York Times* internal network left sensitive databases exposed to hackers, including a file containing Social Security numbers and home phone numbers for contributors to the *Times* op-ed page.

The roster includes Social Security numbers for former U.N. weapons inspector Richard Butler, Democratic party operative James Carville, ex-NSA chief Bobby Inman, "Nannygate" veteran Zoe Baird, former secretary of state James Baker, Internet policy thinker Larry Lessig, and thespian activist Robert Redford, who last May authored an op-ed on President Bush's environmental policies.

Entries with home telephone numbers include Lawrence Walsh, William F. Buckley Jr., Jeanne Kirkpatrick, Rush Limbaugh, Vint Cerf, Warren Beatty and former president Jimmy Carter.

The database includes details on contributors' areas of expertise and what books they've written, and the odd note on how easily they succumb to editing or how much they were paid.

FTC settlement with Eli Lilly

The Federal Trade Commission (FTC) announced a settlement with pharmaceutical giant Eli Lilly after the company inadvertently released the names of nearly 700 Prozac users in an e-mail sent to those users. A source familiar with the talks said that the settlement will not involve Eli Lilly making any cash payments to the FTC.

In the original case, Eli Lilly sent regular e-mail messages to people using its Prozac antidepressant. While the mails were supposed to be sent in a blind carbon copy format, the company accidentally failed to hide the recipients' addresses, which revealed them to all of the other users.

In late June 2001, the company cancelled what it called the Medi-Messenger program whose recipient addresses the Prozac e-mail had disclosed.

Study: Most cyber attacks originate in U.S., Israel

More cyber attacks originate in the United States than in any other country, but the number of attacks that appear to come from Israel is nearly double that of any other nation, according to a recent study from Riptech, a firm that provides security monitoring of corporate and other computer networks.

High-tech, financial services, media/entertainment and power and energy companies showed the highest intensity of attacks per company, each averaging more than 700 attacks per company over the six-month period.

Israel leads the list of countries in terms of number of computer attacks per 10,000 Internet users (26 per 10,000), followed by Hong Kong, Thailand, South Korea, France, Turkey, Malaysia, Poland, Taiwan and Denmark. Only about 3.5 attacks per 10,000 users originated in the U.S.

The study found that power and energy companies were primarily targeted by the Middle East, while high-tech and financial services companies were targeted by Asian attackers.

Information Security Management Office (ISMO)

The Information Security Management Office (ISMO) is a relatively new unit in Technology Services in the Division of Information Services in the Office of Administration. ISMO's primary role is to promote cost effective, consistent and comprehensive information security management in the state. ISMO strives to do this through the adoption of suitable control measures designed to prevent, detect and/or recover from the occurrence of an undesirable event. Below are the unit's Vision and Mission statements.

Vision: To be a leader in preserving the confidentiality, integrity and availability of state data and dependent resources while maintaining efficient and effective operations.

Mission: To promote and provide expertise in information security management for all State agencies; assist local, county or state agencies in the expansion of statewide availability to 9-1-1 and radio interoperability; and support national and local homeland information security efforts.

ISMO has implemented an Incident Response Plan and Procedures to enable efficient and effective responses to information security incidents. A Computer User's Security Guide was developed to inform users of their role in protecting the state's information resources. A logon banner is in the implementation process to remind users of the proper uses for the state's information resources. A Confidentially Agreement is complete and ready for implementation. It will formally document a user's agreement to protect the confidentiality of the state's information resources and comply with information security policies and procedures.

ISMO is currently working on a set of DIS Security Policies. These policies will cover Access Control, Organizational Roles and Responsibilities, Asset Control and Classification, Business Continuity, Compliance and Software and Hardware. At the direction of the ITAB Security Subcommittee a set of statewide policies is also being developed. These policies will cover Acceptable Use, Trusted Networks, Firewall, Network Surveillance, Monitoring and Anti-Cyberterrorism, Incident Handling and Response, Network Certification and Auditing. ISMO has also championed a legislative amendment to the state's Sunshine Law to exempt security information from public disclosure. The current law is not clear on public access to passwords, PIN's and other confidential system security codes.